New Approaches and Experimental Studies on Algebraic Attacks on Stream Ciphers

N Rajesh Pillai

Algebraic attacks constitute an effective class of cryptanalytic attacks which have come up recently. In algebraic attacks, the relations between the input, output and the key are expressed as a system of equations and then solved for the key. The main idea is in obtaining a system of equations which is solvable using reasonable amount of resources. The new approaches proposed in this work and experimental studies on the existing algebraic attacks on stream ciphers will be presented.

In the first attack on filter generator, the input-output relations are expressed in conjunctive normal form. The system of equations is then solved using modified Zakrevskij technique. This was one of the earliest algebraic attacks on the nonlinear filter generator.

In the second attack, we relaxed the constraint on algebraic attack that the entire system description be known and the output sequence extension problem where the filter function is unknown is considered. We modeled the problem as a multivariate interpolation problem and solved it. An advantage of this approach is that it can be adapted to work for noisy output sequences where as the existing algebraic attacks expect the output sequence to be error free.

Adding memory to filter/combiner function increases the degree of system of equations and finding low degree equations in this case is compute-intensive. The method for computing low degree relations for combiners with memory was applied to the combiner in E0 stream cipher. We found that the relation given in literature [Armknecht and Krause] was incorrect. We obtained the correct equation and verified its correctness.

A time-data size trade off attack for clock controlled filter generator was developed. The time complexity and the data requirements are in between the two approaches used in literature.

A recent development of algebraic attacks - the Cube attack was studied. Cube attack on variants of Trivium were proposed by Dinur and Shamir where linear equations in key bits were obtained by combining equations for output bit for same key and a set of Initialization Vectors (IVs). We investigated the effectiveness of the cube attack on Trivium. We showed that the linear equations obtained were not general and hence the attack succeeds only for some specific values of IVs. A reason for the equations not being general is given and a modification to the linear equation finding step suggested.